(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001 年2 月22 日 (22.02.2001)

PCT

(10) 国際公開番号
WO 01/13358 A1

(51) 国際特許分類7: G10K 15/02, G06F 15/00, 17/60, H04L 9/08, 9/32, G06K 19/00, H04H 1/00, H04M 3/42, 3/493, 11/08, G01L 19/00

(21) 国際出願番号: PCT/JP00/05339

(22) 国際出願日: 2000 年8 月9 日 (09.08.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願平11/226406 1999 年8 月10 日 (10.08.1999) JP
特願平11/349336 1999 年12 月8 日 (08.12.1999) JP

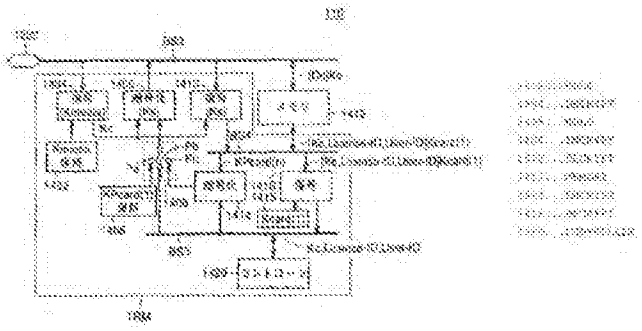
(71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP). 日本コロムビア株式会社 (NIPPON COLUMBIA CO., LTD.) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 Tokyo (JP). 株式会社 日立製作所 (HITACHI, LTD.) [JP/JP]; 〒101-8010 東京都千代田区神田駿河台四丁目6番地 Tokyo (JP). 三洋電機株式会社 (SANYO ELECTRIC CO., LTD.) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 畑中正行 (HATANAKA, Masayuki) [JP/JP]. 蒲田 順 (KAMADA, Jun) [JP/JP]. 畠山卓久 (HATAKEYAMA, Takahisa) [JP/JP]. 長谷部高行 (HASEBE, Takayuki) [JP/JP]. 小谷誠剛 (KOTANI, Seigou) [JP/JP]. 古田茂樹 (FURUTA, Shigeki) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP). 穴澤健明 (ANAZAWA, Takeaki) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 日本コロムビア株式会社内 Tokyo (JP). 利根川

/続葉有/

(54) Title: MEMORY CARD

(54) 発明の名称: メモリカード



(57) Abstract: A memory card (110) extracts a session key (Ks) by decoding data provided on a data bus (BS3). Encryption means (1406) encrypts a public key KPcard (1) of the memory card (110) based on the session key (Ks) and sends it to a server over the data bus (BS3). Each memory (1412) stores data, such as a license key (Kc) encrypted by a unique public key KPcard (1), a license ID, and a user ID, received from the server, and stores content data ([Dc]Kc) encrypted by the license key (Kc) and supplied over the data bus (BS3).

(57) 要約:

メモリカード１１０は、データバスＢＳ３に与えられるデータから、復号処理をすることによりセッションキーＫｓを抽出する。暗号化処理部１４０６は、セッションキーＫｓに基づいて、メモリカード１１０の公開暗号化鍵ＫＰｃａｒｄ（１）を暗号化してデータバスＢＳ３を介してサーバに与える。メモリ１４１２は、メモリカードごとに異なる公開暗号化鍵ＫＰｃａｒｄ（１）で暗号化されているライセンスキーＫｃ、ライセンスＩＤ、ユーザＩＤ等のデータをサーバから受けとって格納し、データバスＢＳ３からライセンスキーＫｃにより暗号化されている暗号化コンテンツデータ［Ｄｃ］Ｋｃを受けて格納する。

WO 01/13358 A1

忠明 (TONEGAWA, Tadaaki) [JP/JP]; 〒187-8588 東京都小平市上水本町五丁目20番1号 株式会社 日立製作所 半導体グループ内 Tokyo (JP). 日置敏昭 (HIOKI, Toshiaki) [JP/JP]. 金森美和 (KANAMORI, Miwa) [JP/JP]. 堀　吉宏 (HORI, Yoshihiro) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内Osaka (JP).

(74) 代理人：深見久郎、外(FUKAMI, Hisao et al.); 〒530-0054 大阪府大阪市北区南森町2丁目1番29号 住友銀行南森町ビル Osaka (JP).

(81) 指定国(国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) 指定国(広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

明細書

メモリカード

技術分野

本発明は、携帯電話等の端末に対して情報を配送するための情報配信システムにおいて、コピーされた情報に対する著作権保護を可能とするメモリカードに関するものである。

背景技術

近年、インターネット等の情報通信網等の進歩により、携帯電話等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

このような情報通信においてはデジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像情報を各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、情報のコピーを行なうことが可能である。

したがって、このような情報通信網上において、音楽情報や画像情報等の著作権の存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物の複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタル情報を記録した記録媒体を例にとって考えてみると、通常販売されている音楽情報を記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行な

う個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して補償金として支払うことになっている。

しかも、CDからMDへデジタル信号である音楽情報をコピーした場合、これらの情報がコピー劣化のほとんどないデジタル情報であることに鑑み、1つのMDからさらに他のMDに音楽データをデジタル情報としてコピーすることは、著作権者保護のために機器の構成上できないようになっている。

すなわち、現状においては、デジタル記録媒体であるCDからMDへのコピーは、自由に行なうことができるものの、記録可能なMDからMDへのコピーを行なうことはできない。

そのような事情からも、音楽情報や画像情報をデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

この場合、情報通信網を通じて公衆に送信される著作物データを、本来受信する権原のないユーザが受信することを防止する必要があるのはもちろんのこと、仮に権原を有するユーザが受信を行なった場合でも、一度受信された著作物が、さらに勝手に複製されることを防止することも必要となる。

発明の開示

本発明の目的は、情報通信網、たとえば携帯電話等の情報通信網を介して著作物データを配信する場合に、正当なアクセス権を有するユーザのみがこのような情報を受信することが可能な情報配信システムにおけるメモリカードを提供することである。

この発明の他の目的は、配信された著作物データが、著作権者の許可なく複製されることを防止することが可能な情報配信システムにおけるメモリカードを提供することである。

係る目的を達成するために本願発明に係るメモリカードは、暗号化コンテンツデータを受けて記録するためのメモリカードであって、第1の鍵保持部と、第1の復号処理部と、第2の鍵保持部と、第1の暗号化処理部と、第2の復号処理部と、第1の記憶部と、第3の鍵保持部と、第3の復号処理部とを備える。

第１の鍵保持部は、メモリカードに対応して予め定められた第１の公開暗号化鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する。

第１の復号処理部は、暗号化コンテンツデータの通信ごとに更新されて配信され、第１の公開暗号化鍵によって暗号化された第１の共通鍵を受けて、復号処理する。

第２の鍵保持部は、メモリカードごとに異なる第２の公開暗号化鍵を保持する。第１の暗号化処理部は、第２の公開暗号化鍵を、第１の共通鍵に基づいて暗号化し、出力する。

第２の復号処理部は、第２の公開暗号化鍵で暗号化され、さらに第１の共通鍵で暗号化されたコンテンツキーを受け、第１の共通鍵に基づいて復号化する。第１の記憶部は、第２の復号処理部の出力を受けて、格納する。第３の鍵保持部は、第２の公開暗号化鍵によって暗号化されたデータを復号化するための第２の秘密復号鍵を保持する。第３の復号処理部は、第１の記憶部に格納されたデータに基づいて、第２の秘密復号鍵によりコンテンツキーを復号する。

本発明の他の局面に従うと、暗号化データと暗号化データを復号するための復号情報データを受けて記録するためのメモリカードであって、第１の記憶部と、第１の鍵保持部と、第２の鍵保持部と、第１の復号処理部と、第３の鍵保持部と、セッションキー発生部と、第１の暗号化処理部と、第２の復号処理部と、第２の記憶部と、第４の鍵保持部と、第３の復号処理部とを備える。

第１の記憶部は、暗号化データを格納する。第１の鍵保持部は、メモリカードに対応して予め定められた第１の公開暗号化鍵と自身の認証データとを公開認証鍵により復号できるように暗号化して保持し、外部に対して出力可能である。

第２の鍵保持部は、第１の公開暗号化鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する。第１の復号処理部は、復号情報データの通信ごとに更新されて送信され、第１の公開暗号化鍵によって暗号化された第１の共通鍵を受けて、復号処理する。

第３の鍵保持部は、メモリカードごとに異なる第２の公開暗号化鍵を保持する。

セッションキー発生部は、復号情報データの通信ごとに更新される第２の共通鍵を生成する。第１の暗号化処理部は、第２の公開暗号化鍵と第２の共通鍵を、

第１の共通鍵に基づいて暗号化し、出力する。第２の復号処理部は、外部にて第２の公開暗号鍵によって暗号化され、さらに第２の共通鍵によって暗号化された復号情報データを第２の共通鍵に基づいて復号する。

第２の記憶部は、第２の復号処理部の出力である第２の公開暗号鍵によって暗号化された復号情報データを格納する。第４の鍵保持部は、第２の公開暗号化鍵によって暗号化されたデータを復号するための第２の秘密復号鍵を保持する。第３の復号処理部は、第２の記憶部に格納されたデータを第２の秘密復号鍵に基づいて復号し、復号情報データを抽出する。

この発明のさらに他の局面に従うと、暗号化データと暗号化データを復号するための復号情報データを受けて記録するためのメモリカードであって、第１の記憶部と、第１の鍵保持部と、第２の鍵保持部と、第１の復号処理部と、第３の鍵保持部と、セッションキー発生部と、第１の暗号化処理部と、第２の復号処理部と、第４の鍵保持部と、第３の復号処理部と、第２の記憶部とを備える。

第１の記憶部は、暗号化データを格納する。第１の鍵保持部は、メモリカードに対応して予め定められた第１の公開暗号化鍵と自身の認証データとを公開認証鍵により復号できるように暗号化して保持し、外部に対して出力可能である。

第２の鍵保持部は、第１の公開暗号化鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する。第１の復号処理部は、復号情報データの通信ごとに更新されて送信され、第１の公開暗号化鍵によって暗号化された第１の共通鍵を受けて、復号処理する。第３の鍵保持部は、メモリカードごとに異なる第２の公開暗号化鍵を保持する。

セッションキー発生部は、復号情報データの通信ごとに更新される第２の共通鍵を生成する。第１の暗号化処理部は、第２の公開暗号化鍵と第２の共通鍵を、第１の共通鍵に基づいて暗号化し、出力する。

第２の復号処理部は、外部にて第２の公開暗号鍵によって暗号化され、さらに第２の共通鍵によって暗号化された復号情報データを第２の共通鍵に基づいて復号する。

第４の鍵保持部は、第２の公開暗号化鍵によって暗号化されたデータを復号化するための第２の秘密復号鍵を保持する。

第３の復号処理部は、外部にて第２の公開暗号化鍵によって暗号化された復号情報データを受けて、第２の秘密復号鍵により復号情報データを復号する。第２の記憶部は、復号情報データを格納する。

したがって、本発明によれば、正規のユーザのみがコンテンツデータを受信してメモリ中に格納することが可能となり、かつ、１度メモリカード中に格納されたデータを、他人にコピーさせる場合は、当該他人が再生可能な状態でデータを移植するためには、送信元においては、データの再生が不能となってしまう構成となっているので、無制限なコピーにより著作権が不当な不利益を被るのを防止することが可能となる。

図面の簡単な説明

図１は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

図２は、図１に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明する図である。

図３は、図１に示したコンテンツサーバ１０の構成を示す概略ブロック図である。

図４は、図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。

図５は、図４に示したメモリカード１１０の構成を説明するための概略ブロック図である。

図６は、図１および図３～図５で説明したデータ配信システムにおける配信モードを説明するためのフローチャートである。

図７は、実施例１の暗号化コンテンツデータを復号し音楽データとして出力する再生モードを説明するフローチャートである。

図８は、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なうモードを説明するためのフローチャートである。

図９は、暗号化されたコンテンツデータの複製を行なうモードを説明するためのフローチャートである。

図１０は、本発明の実施例２のメモリカード１３０の構成を説明するための概略ブロック図である。

図１１は、メモリカード１３０の移動モードを説明するためのフローチャートである。

図１２は、本発明の実施例３のメモリカード１４０の構成を説明するための概略ブロック図である。

図１３は、図１２で説明したメモリカード１４０を用いた配信モードを説明するためのフローチャートである。

図１４は、実施例３の暗号化コンテンツデータを復号し音楽データとして出力する再生モードを説明するフローチャートである。

図１５は、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なう処理を説明するためのフローチャートである。

図１６は、暗号化されたコンテンツデータの複製を行なうモードを説明するためのフローチャートである。

図１７は、実施例３の変形例の暗号化コンテンツデータを復号し音楽データとして出力する再生モードを説明するフローチャートである。

図１８は、本発明の実施例４のメモリカード１５０の構成を説明するための概略ブロック図である。

図１９は、メモリカード１５０の移動モードを説明するためのフローチャートであり、実施例２の図１１と対比される図である。

図２０は、本発明の実施例５のメモリカード１６０の構成を説明するための概略ブロック図である。

図２１は、図２０で説明したメモリカード１６０を用いた配信モードを説明するためのフローチャートである。

図２２は、実施例５の暗号化コンテンツデータを復号し音楽データとして出力する再生モードを説明するフローチャートである。

図２３は、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なうモードを説明するためのフローチャートである。

図２４は、本発明の実施例６のメモリカード１７０の構成を説明するための概

略ブロック図である。

図２５は、メモリカード１７０の移動モードを説明するためのフローチャートである。

図２６は、実施例７の携帯電話機１０１の構成を説明するための概略ブロック図である。

図２７は、実施例７のメモリカード１８０に対応したコンテンツサーバ１１の構成を示す概略ブロック図である。

図２８は、本発明の実施例７のメモリカード１８０の構成を説明するための概略ブロック図である。

図２９は、本発明の実施例７のメモリカード１８０を用いた配信モードを説明するためのフローチャートである。。

図３０は、実施例７の暗号化コンテンツデータを復号し音楽データとして出力する再生モードを説明するフローチャートである。

図３１は、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なうモードを説明するためのフローチャートである。

図３２は、実施例８における携帯電話機１０５の構成を説明するための概略ブロック図である。

図３３は、実施例８のメモリカード１９０に対応したコンテンツサーバ１２の構成を示す概略ブロック図である。

図３４は、本発明の実施例８のメモリカード１９０の構成を説明するための概略ブロック図である。

図３５は、実施例８のメモリカード１９０の記録領域の配置を示す概略図である。

図３６は、図３５で説明したメモリカード１９０を用いた配信モードを説明するためのフローチャートである。

図３７は、メモリカード１９０に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生モードを説明するフローチャートである。

図３８は、実施例８の２つのメモリカード間において、移動を行なう処理を説明するためのフローチャートである。

図３９は、実施例９のメモリカード２００の構成を示す概略ブロック図である。

図４０は、実施例９のメモリカード２００の記録領域の配置を示す概略ブロック図である。

図４１は、図３８で説明したメモリカード２００を用いた配信モードを説明するためのフローチャートである。

図４２は、メモリカード２００に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生モードを説明するフローチャートである。

図４３は、実施例９の２つのメモリカード間において、移動を行なうモードを説明するためのフローチャートである。

発明を実施するための最良の形態

以下、本発明の実施例を図面とともに説明する。

〔実施例１〕

図１は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

なお、以下では携帯電話網を介して、音楽データを各ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物データ、たとえば画像データ等の著作物データを、他の情報通信網を介して配信する場合にも適用することが可能なものである。

図１を参照して、著作権の存在する音楽情報を管理するコンテンツサーバ１０は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化したうえで、情報を配信するための配信キャリア２０である携帯電話会社に、このような暗号化データを与える。

配信キャリア２０は、自己の携帯電話網を通じて、各ユーザからの配信要求（配信リクエスト）をコンテンツサーバ１０に中継する。コンテンツサーバ１０は配線リクエストに応じて、要求されたコンテンツデータをさらに暗号化したうえで、配信キャリア２０の携帯電話網を介して、各ユーザの携帯電話機に対して配信する。

図１においては、たとえば携帯電話ユーザ１の携帯電話機１００には、携帯電話１００により受信された暗号化されたコンテンツデータを受取って、上記送信にあたって行なわれた暗号化については復号化したうえで、携帯電話機１００中の音楽再生部（図示せず）に与えるための着脱可能なメモリカード１１０に格納する構成となっている。

さらに、たとえばユーザ１は、携帯電話機１００に接続したヘッドホン１３０等を介してこのようなコンテンツデータを再生した音楽を聴取することが可能である。

以下では、このようなコンテンツサーバ１０と配信キャリア２０とを併せて、音楽サーバ３０と総称することにする。

また、このような音楽サーバ３０から、各携帯電話端末にコンテンツデータを伝送する処理を「配信」と称することとする。

このような構成とすることで、まず、正規のメモリカードであるメモリカード１１０を購入していないユーザは、音楽サーバ３０からの配信データを受取って再生することが困難な構成となる。

しかも、配信キャリア２０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話の通話料金として徴収することとすれば、著作権者が著作権料を確保することが容易となる。

しかも、このようなコンテンツデータの配信は、携帯電話網というクローズドなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

このとき、たとえばメモリカード１１２を有するユーザ２が、自己の携帯電話機１０２により、音楽サーバ３０から直接コンテンツデータの配信を受けることは可能である。しかしながら、相当量の情報量を有するコンテンツデータ等をユーザ２が直接音楽サーバ３０から受信することとすると、その受信のために比較的長い時間を要してしまう場合がある。このような場合、既に当該コンテンツデータの配信を受けているユーザ１から、そのコンテンツデータをコピーできるこ

とを可能としておけば、ユーザにとっての利便性が向上する。

しかしながら、著作権者の権利保護の観点からは、自由なコンテンツデータのコピーを放任することはシステム構成上許されない。

図１に示した例では、ユーザ１が受信したコンテンツデータを、コンテンツデータそのものおよび当該コンテンツデータを再生可能とするために必要な情報とともに、ユーザ２に対してコピーさせる場合をコンテンツデータの「移動」と呼ぶ。この場合、ユーザ１は、再生のために必要な情報（再生情報）ごとユーザ２にコピーさせるため、情報の移動を行なった後には、ユーザ１においてはコンテンツデータの再生を行なうことは不可能とする必要がある。ここで、コンテンツデータとは所定の暗号化方式に従って暗号化された暗号化コンテンツデータとして配信され、「再生情報」とは、後に説明するように、上記所定の暗号化方式にしたがって暗号化されたコンテンツデータを復号可能なライセンスキーと、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤ等のライセンス情報とを意味する。

これに対して、コンテンツデータのみを暗号化されたままの状態で、ユーザ２にコピーさせることを音楽情報の「複製」と呼ぶこととする。

この場合、ユーザ２の端末には、このようなコンテンツデータを再生させるために必要な再生情報はコピーされないので、ユーザ２は、暗号化されたコンテンツデータを得ただけでは、音楽を再生させることができない。したがって、ユーザ２が、このような音楽の再生を望む場合は、改めて音楽サーバ３０からコンテンツデータの再生を可能とするための再生情報の配信を受ける必要がある。しかしながら、この場合は、再生を可能とするための情報の配信のみを受ければよいため、ユーザ２が直接音楽サーバ３０からすべての配信を受ける場合に比べて、格段に短い通話時間で、音楽再生を可能とすることができる。

たとえば、携帯電話機１００および１０２が、ＰＨＳ（Personal Handy Phone）（登録商標）である場合には、いわゆるトランシーバモードの通話が可能となっているので、このような機能を利用して、ユーザ１からユーザ２への一括した情報の移転（移動）や、暗号化したコンテンツデータのみの転送（複製）を行なうことが可能である。

図１に示したような構成においては、暗号化して配信されるコンテンツデータをユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信における暗号化キー（鍵）を配送するための方式であり、さらに第２には、配信データを暗号化する方式そのものであり、さらに、第３には、このようにして配信されたデータの無断コピーを防止するためのデータ保護を実現する構成である。

図２は、図１に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

まず、図１に示した構成において、メモリカード１００内のデータ処理を管理するための鍵としては、メモリカードという媒体の種類に固有で、すべてのメモリカードに対して共通な秘密復号鍵Ｋｍｅｄｉａと、メモリカードごとに異なる公開暗号化鍵ＫＰｃａｒｄ（ｎ）と、公開暗号化鍵ＫＰｃａｒｄ（ｎ）により暗号化されたデータを復号するための秘密復号鍵Ｋｃａｒｄ（ｎ）とがある。

ここで、秘密復号鍵Ｋｃａｒｄ（ｎ）や秘密復号鍵ＫＰｃａｒｄ（ｎ）の表記中の自然数ｎは、各ユーザ（メモリカード）を区別するための番号を表わす。

すなわち、公開暗号化鍵ＫＰｃａｒｄ（ｎ）で暗号化されたデータは、各メモリカードごとに存在する秘密復号鍵Ｋｃａｒｄ（ｎ）で復号可能である。したがって、メモリカードにおける配信データの授受にあたっては、基本的には、後に説明するように３つの鍵Ｋｍｅｄｉａ、Ｋｃａｒｄ（ｎ）、ＫＰｃａｒｄ（ｎ）が用いられることになる。

さらに、メモリカード外とメモリカード間でのデータの授受における秘密保持のための暗号鍵としては、各媒体に固有、すなわち、メモリカードすべてに共通な公開暗号化鍵ＫＰｍｅｄｉａと、公開暗号化鍵ＫＰｍｅｄｉａにより暗号化されたデータを復号化するための秘密復号鍵Ｋｍｅｄｉａと、各通信ごと、たとえば、音楽サーバ３０へのユーザのアクセスごとに生成される共通鍵Ｋｓが用いられる。

ここで、共通鍵Ｋｓは、上述のとおり、ユーザが音楽サーバ３０に対して１回のアクセスを行なうごとに発生する構成として、１回のアクセスである限り何曲の音楽情報についても同一の共通鍵が用いられる構成としてもよいし、また、た

とえば、各曲目ごとにこの共通鍵を変更したうえでその都度ユーザに配信する構成としてもよい。

以下では、このような通信の単位あるいはアクセスの単位を「セッション」と呼ぶことにし、共通鍵Ｋｓを「セッションキー」とも呼ぶことにする。

したがって、共通鍵Ｋｓは各通信セッションに固有の値を有することになり、配信サーバや携帯電話機において管理される。

また、配信されるべきデータについては、まず、暗号化されたコンテンツデータを復号する鍵であるＫｃ（以下、ライセンスキーと呼ぶ）があり、このライセンス鍵Ｋｃにより暗号化されたコンテンツデータが復号化されるものとする。さらに、当該コンテンツデータを特定できる管理コードや、再生を行なう回数の制限などの情報を含むライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤと、受信者を識別するためのユーザＩＤデータ User－ＩＤ等が存在する。ここで、ユーザＩＤデータ User－ＩＤとしては、たとえばユーザの電話番号等を用いることが可能である。

このような構成とすることで、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤに含まれる情報に応じて、著作権者側の著作権保護に関する制御を行なうことが可能であり、一方ユーザＩＤデータ User－ＩＤを用いることで、ユーザの個人情報の保護、たとえばユーザのアクセス履歴等が部外者から知ることができないように保護するといったような制御を行なうことが可能である。

配信データにおけるコンテンツデータＤｃは、上述のとおり、たとえば音楽データであり、このコンテンツデータをライセンスキーＫｃで復号化可能なデータを、暗号化コンテンツデータ［Ｄｃ］Ｋｃと呼ぶ。

ここで、［Ｙ］Ｘという表記は、データＹを、キーＸにより復号可能な暗号に変換した情報であることを示している。

図３は、図１に示したコンテンツサーバ１０の構成を示す概略ブロック図である。コンテンツサーバ１０は、コンテンツデータ（音楽データ）を所定の方式に従って暗号化したデータや、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ等の配信情報を保持するための配信情報データベース３０４と、各ユーザごとにコンテンツデータへのアクセス回数等に従った課金情報を保持するための課金データベ

ース３０２と、配信情報データベース３０４および課金データベース３０２からのデータをデータバスＢＳ１を介して受取り、所定の暗号化処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

データ処理部３１０は、データバスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１２と、配信制御部３１２に制御されて、セッションキーＫｓを発生するためのセッションキー発生部３１４と、セッションキー発生部３１４より生成されたセッションキーＫｓを、公開暗号化鍵ＫＰｍｅｄｉａにより暗号化して、データバスＢＳ１に与えるための暗号化処理部３１６と、各ユーザの携帯電話機においてセッションキーＫｓにより暗号化されたうえで送信されたデータを通信装置３５０およびデータバスＢＳ１を介して受けて、復号処理を行なう復号処理部３１８と、復号処理部３１８により抽出された公開暗号化鍵ＫＰｃａｒｄ（ｎ）を用いて、ライセンスキーやライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ等のデータを配信制御部３１２に制御されて暗号化するための暗号化処理部３２０と、暗号化処理部３２０の出力を、さらにセッションキーＫｓにより暗号化して、データバスＢＳ１を介して通信装置３５０に与える暗号化処理部３２２とを含む。

図４は、図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。

携帯電話機１００は、携帯電話網により無線伝送される信号を受信するためのアンテナ１１０２と、アンテナ１１０２からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ１１０２に与えるための送受信部１１０４と、携帯電話機１００の各部のデータ授受を行なうためのデータバスＢＳ２と、データバスＢＳ２を介して携帯電話機１００の動作を制御するためのコントローラ１１０６と、外部からの指示を携帯電話機１００に与えるためのタッチキー部１１０８と、コントローラ１１０６等から出力される情報をユーザに視覚情報として与えるためのディスプレイ１１１０と、通常の通話モードにおいて、データバスＢＳ２を介して与えられる受信データに基づいて音声を再生するための音声再生部１１１２とを備える。

携帯電話機１００は、さらに、コンテンツサーバ１０からのコンテンツデータを復号化処理するための着脱可能なメモリカード１１０と、メモリカード１１０とデータバスＢＳ２との間のデータの授受を制御するためのメモリインタフェース１２００と、メモリカード１１０と携帯電話機の他の部分とのデータ授受にあたり、データバスＢＳ２上においてやり取りされるデータを暗号化するためのセッションキーＫｓを乱数等により発生するセッションキー発生部１５０２と、セッションキー発生部１５０２により生成されたセッションキーを公開暗号化鍵ＫＰｍｅｄｉａで暗号化して、データバスＢＳ２に与えるための暗号化処理部１５０４と、セッションキー発生部１５０２において生成されたセッションキーＫｓに基づいて、データバスＢＳ２上のデータをセッションキーＫｓにより復号して出力する復号処理部１５０６と、復号処理部１５０６の出力を受けて、音楽信号を再生するための音楽再生部１５０８と、音楽再生部１５０８の出力と音声再生部１１１２の出力とを受けて、動作モードに応じて選択的に出力するための混合部１５１０と、混合部１５１０の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部１５１２と、デジタルアナログ変換部１５１２の出力を受けて、ヘッドホン１２０と接続するための接続端子１５１４とを含む。

なお、説明の簡素化のため本発明のコンテンツデータの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

図５は、図４に示したメモリカード１１０の構成を説明するための概略ブロック図である。

メモリカード１１０は、メモリインタフェース１２００との間で信号を端子１２０２を介して授受するデータバスＢＳ３と、秘密復号鍵Ｋｍｅｄｉａを保持するためのＫｍｅｄｉａ保持部１４０２と、データバスＢＳ３にメモリインタフェース１２００から与えられるデータから、秘密復号鍵Ｋｍｅｄｉａにより復号処理をすることにより、セッションキーＫｓを抽出する復号処理部１４０４と、公開暗号化キーＫＰｃａｒｄ（１）を保持するためのＫＰｃａｒｄ（１）保持部１４０５と、復号処理部１４０４により抽出されたセッションキーＫｓに基づいて、

切換えスイッチ１４０８からの出力を暗号化してデータバスＢＳ３に与えるための暗号化処理部１４０６と、データバスＢＳ３上のデータを復号処理部１４０４により抽出されたセッションキーＫｓにより復号処理してデータバスＢＳ４に与えるための復号処理部１４１０と、データバスＢＳ４からメモリカードごとに異なる公開暗号化鍵ＫＰｃａｒｄ（ｎ）で暗号化されているライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤ等のデータを格納し、データバスＢＳ３からライセンスキーＫｃにより暗号化されている暗号化コンテンツデータ［Ｄｃ］Ｋｃを受けて格納するためのメモリ１４１２とを備える。

切換えスイッチ１４０８は、接点Ｐａ、Ｐｂ、Ｐｃを有し、接点ＰａにはＫＰｃａｒｄ（１）保持部１４０５からの暗号化キーＫＰｃａｒｄ（１）が、接点ＰｂにはデータバスＢＳ５が、接点Ｐｃには暗号化処理部１４１４の出力が与えられる。切換えスイッチ１４０８は、それぞれ、接点Ｐａ、Ｐｂ、Ｐｃに与えられる信号を、動作モードが、「配信モード」、「再生モード」、「移動モード」のいずれであるかに応じて、選択的に暗号化処理部１４０６に与える。

メモリカード１１０は、さらに、秘密復号キーＫｃａｒｄ（１）の値を保持するためのＫｃａｒｄ（１）保持部１４１５と、公開暗号化鍵ＫＰｃａｒｄ（１）により暗号化されており、かつ、メモリ１４１２から読出されたライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤ等（［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（１））を、復号処理してデータバスＢＳ５に与える復号処理部１４１６と、データの移動処理等において、相手先のメモリカードの公開暗号化鍵ＫＰｃａｒｄ（ｎ）を復号処理部１４１０から受けて、この相手方の公開暗号化鍵ＫＰｃａｒｄ（ｎ）に基づいて、データバスＢＳ５上に出力されているライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤ等を暗号化したうえで、切換えスイッチ１４０８に出力するための暗号化処理部１４１４と、データバスＢＳ５との間でライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤ等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０とを備える。

なお、図５において実線で囲んだ領域は、メモリカード１１０内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読み出しを不能化するためのモジュールＴＲＭに組込まれているものとする。

このようなモジュールは、一般にはタンパーレジスタンスモジュール（Tamper Resistance Module）と呼ばれる。

もちろん、メモリ１４１２も含めて、モジュールＴＲＭ内に組み込まれる構成としてもよい。しかしながら、図５に示したような構成とすることで、メモリ１４１２中に保持されているデータは、いずれも暗号化されているデータであるため、第三者はこのメモリ１４１２中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタンスモジュール内にメモリ１４１２を設ける必要がないので、製造コストが低減されるという利点がある。

図６は、図１および図３～図５で説明したデータ配信システムにおける配信モードを説明するためのフローチャートである。

図６においては、ユーザ１が、メモリカード１１０を用いることで、コンテンツサーバ１０からコンテンツデータの配信を受ける場合の動作を説明している。

まず、ユーザ１の携帯電話機１００から、ユーザのキーボタンの操作等によって、コンテンツサーバ１０に対して配信リクエストがなされる（ステップＳ１００）。

コンテンツサーバ１０においては、この配信リクエストに応じて、セッションキー発生部３１４が、セッションキーＫｓを生成する（ステップＳ１０３）。

続いて、サーバ内の暗号化処理部３１６が、公開暗号化キーＫＰｍｅｄｉａにより、セッションキーＫｓを暗号化処理して、データバスＢＳ１に与える（ステップＳ１０４）。

通信装置３５０は、暗号化処理部３１６からの暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａを、通信網を通じて、携帯電話機１００のメモリカード１１０に対して送信する（ステップＳ１０６）。

メモリカード１１０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた受信データを、復号処理部１４０４が、Ｋｍｅｄｉ

ａ保持部１４０２から与えられる秘密復号キーＫｍｅｄｉａにより復号処理することにより、セッションキーＫｓを復号し抽出する（ステップＳ１０８）。

続いて、配信モードにおいては、切換えスイッチ１４０８は、接点Ｐａが閉じる状態が選択されているので、暗号化処理部１４０６は、接点Ｐａを介してＫＰｃａｒｄ（１）保持部１４０５から与えられる公開暗号化鍵ＫＰｃａｒｄ（１）（ユーザ１のメモリカードにおける公開暗号化鍵）を、セッションキーＫｓにより暗号化して、データバスＢＳ３に与える（ステップＳ１１０）。

携帯電話機１００は、暗号化処理部１４０６により暗号化されたデータ［ＫＰｃａｒｄ（１）］Ｋｓをコンテンツサーバ１０に対して出力する（ステップＳ１１２）。

コンテンツサーバ１０では、通信装置３５０により受信され、データバスＢＳ１に与えられたデータ［ＫＰｃａｒｄ（１）］Ｋｓを復号処理部３１８が、セッションキーＫｓにより復号化処理して、公開暗号化キーＫＰｃａｒｄ（１）を復号抽出する（ステップＳ１１４）。

続いて、配信制御部３１２は、ライセンスキーＫｃを配信情報データベース３０４より取得し（ステップＳ１１６）、かつ、配信情報データベース３０４等に保持されているデータを元に、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータ User－ＩＤ等のライセンス情報を生成する（ステップＳ１１８）。

暗号化処理部３２０は、配信制御部３１２からのライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータ User－ＩＤ等のデータを受取って、復号処理部３１８より与えられた公開暗号化キーＫＰｃａｒｄ（１）により暗号化処理する（ステップＳ１２０）。

暗号化処理部３２２は、暗号化処理部３２０により暗号化されたデータを受取って、さらにセッションキーＫｓにより暗号化して、データバスＢＳ１に与える（ステップＳ１２２）。

通信装置３５０は、暗号化処理部３２２により暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（１）］Ｋｓをカード１１０に対して送信する。

メモリカード１１０においては、復号処理部１４１０がセッションキーＫｓにより、復号処理を行ない、データ［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（１）を抽出し（ステップＳ１２６）、メモリ１４１２に格納する（ステップＳ１２８）。

一方、コンテンツサーバ１０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを配信情報データベース３０４より取得して、通信装置３５０を介して、メモリカード１１０に送信する（ステップＳ１３０）。

メモリカード１１０においては、受信したデータ［Ｄｃ］Ｋｃをそのままメモリ１４１２に格納する（ステップＳ１３２）。

以上のような動作により、メモリカード１１０が格納するコンテンツデータは再生可能な状態となるので、以下では，メモリカードが格納するコンテンツデータが再生可能な状態となっていることを、「メモリカード１１０は、状態ＳＡにある」と呼ぶことにする。

図７は、携帯電話機１００内において、メモリカード１１０に保持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

図７を参照して、携帯電話機１００のタッチキー１１０８等からのユーザ１の指示により、再生リクエストがメモリカード１１０に対して出力される（ステップＳ２００）。

メモリカード１１０では、メモリ１４２０から、暗号化されているライセンスキーKc、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤ等を読出し（ステップＳ２０３）、秘密復号キーＫｃａｒｄ（１）によって、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤやユーザＩＤデータ User－ＩＤを復号処理する（ステップＳ２０４）。

コントローラ１４２０は、復号化されたライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ等に含まれる情報に基づいて、復号可能なデータに対するリクエストであるかを判断し（ステップＳ２０６）、復号可能と判断した場合は、携帯電話機のコントローラ１１０６に対して、再生許可通知を送信する（ステップＳ２０８）。

携帯電話機１００においては、セッションキー発生回路１５０２がセッション

キーＫｓを生成し（ステップＳ２１０）、暗号化処理部１５０４が、公開暗号化キーＫＰｍｅｄｉａによりセッションキーＫｓを暗号化して（ステップＳ２１２）、データバスＢＳ２に暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａが出力される（ステップＳ２１４）。

メモリカード１１０は、データバスＢＳ２を介して、携帯電話機１００により生成された暗号化セッションキーを受け取り、秘密復号キーＫｍｅｄｉａにより復号し抽出する（ステップＳ２１６）。

続いて、メモリカード１１０は、抽出したセッションキーＫｓにより、ライセンスキーＫｃを暗号化し（ステップＳ２１９）、暗号化ライセンスキー［Ｋｃ］Ｋｓをデータバスに与える（ステップＳ２２０）。

携帯電話機１００の復号処理部１５０６は、セッションキーＫｓにより復号化処理を行なうことにより、ライセンスキーＫｃを取得する（ステップＳ２２２）。

続いて、メモリカード１１０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読出し、データバスＢＳ２に与える（ステップＳ２２４）。

携帯電話機１００の音楽再生部１５０８は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを、抽出されたライセンスキーＫｃにより復号処理し（ステップＳ２２６）、コンテンツデータを再生して混合部１５１０に与える（ステップＳ２２８）。

一方、ステップＳ２０６において、コントローラ１４２０が復号処理は不可能であると判断した場合、メモリカード１１０は、携帯電話機１００に対して、再生不許可通知を送信する（ステップＳ２３０）。

ステップＳ２３０の状態では、コンテンツデータの再生を行なうことができないので、このような状態を以下では「メモリカード１１０は、状態ＳＢにある」と表現することにする。

図８は、２つのメモリカード間において、コンテンツデータおよび再生情報の移動を行なう処理を説明するためのフローチャートである。

まず、携帯電話機１００が送信側であり、携帯電話機１０２が受信側であるものとする。

携帯電話機１００は、まず、自身の側のメモリカード１１０と、受信側の携帯電話機１０２に挿入されたメモリカード１１２に対して、移動リクエストを出力

する（ステップＳ３００）。

さらに、携帯電話機１００においては、セッションキー発生回路１５０２は、セッションキーＫｓを生成し（ステップＳ３０３）、公開暗号化キーＫＰｍｅｄｉａを用いて、暗号化処理部１５０４がセッションキーＫｓを暗号化し（ステップＳ３０４）、その暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａをデータバス ＢＳ２を介して、メモリカード１１０に伝達するとともに、携帯電話機１０２に装着されたメモリカード１１２に対して、たとえば、トランシーバモードではアンテナ１１０２を介して、上記暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａを伝達する（ステップＳ３０６）。

メモリカード１１０においては、秘密復号キーＫｍｅｄｉａによりセッションキーＫｓを復号抽出する（ステップＳ３１８）。

同様にして、カード１１２においても、秘密復号キーＫｍｅｄｉａにより、セッションキーＫｓを復号抽出し（ステップＳ３２０）、さらに、セッションキーＫｓによりメモリカード１１２の公開暗号化キーＫＰｃａｒｄ（２）を暗号化して（ステップＳ３２２）、メモリカード１１０に対して、暗号化されたデータ［ＫＰｃａｒｄ（２）］Ｋｓを送信する（ステップＳ３２４）。

メモリカード１１０においては、メモリカード１１２から送信された暗号化データをセッションキーＫｓにより復号化して、メモリカード１１２の公開暗号化キーＫＰｃａｒｄ（２）を復号抽出する（ステップＳ３２６）。

続いて、メモリカード１１０においては、メモリ１４１２からメモリカード１１０の公開暗号化キーＫｃａｒｄ（１）により暗号化されているライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータ User－ＩＤが読出される（ステップＳ３２８）。

続いて、復号処理部１４１６が、秘密復号キーＫｃａｒｄ（１）により、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤとを復号処理する（ステップＳ３３０）。

さらに、暗号化処理部１４１４は、復号処理部１４１０において抽出されたカードＩ１２における公開暗号化キーＫＰｃａｒｄ（２）により、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－

ＩＤとを暗号化する（ステップＳ３３２）。

暗号化処理部１４１４により暗号化されたデータは、切換えスイッチ１４０８（接点Ｐｃが閉じている）を介して、さらに、暗号化処理部１４０６に与えられ、暗号化処理部１４０６は、データ［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（２）をセッションキーＫｓにより暗号化する（ステップＳ３３４）。

続いて、メモリカード１１０は、携帯電話機１００を介して、メモリカード１１２に対して、暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（２）］Ｋｓを送信する（ステップＳ３３６）。

メモリカード１１２においては、メモリカード１１０から送信されたデータを復号処理部１４１０により、セッションキーＫｓに基づいて復号化処理して（ステップＳ３３８）、メモリ１４１２に格納する（ステップＳ３４０）。

一方、メモリカード１１０は、さらに、メモリ１４１２内のデータのうち、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータUser－ＩＤに対応したデータを消去する（ステップＳ３４２）。

続いて、メモリカード１１０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリから読出し、メモリカード１１２に対して送信する（ステップＳ３４４）。

メモリカード１１２は、受信した暗号化コンテンツデータをそのままメモリ１４１２に格納する（ステップＳ３４６）。

以上のような処理を行なうと、ステップＳ３４２において、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータ User－ＩＤ等がメモリカード１１０からは消去されているので、メモリカード１１０は「状態ＳＢ」となる。

一方、メモリカード１１２においては、暗号化コンテンツデータ以外にも、ライセンスキー、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータUser－ＩＤ等のすべてのデータが移動されているので、メモリカード１１２は「状態ＳＡ」となっている。

図９は、図１に示した情報配信システムにおいて、携帯電話機１００から携帯電話機１０２へ、暗号化コンテンツデータの複製を行なう処理を説明するための

フローチャートである。

図９を参照して、携帯電話機１００が、メモリカード１１０およびメモリカード１１２に対して複製リクエストを出力する（ステップＳ４００）。

続いて、メモリカード１１０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読出し、メモリカード１１２に対して出力する（ステップＳ４０２）。

メモリカード１１２においては、メモリカード１１０から送信された暗号化されたコンテンツデータを、そのままメモリ１４１２に記録する（ステップＳ４０４）。

以上のような動作を行なうと、メモリカード１１０には、暗号化コンテンツデータ、ライセンスキーＫｃ、ユーザＩＤデータ User－ＩＤ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ等のすべてのデータが残されているため、メモリカード１１０は再生可能な状態、すなわち、「状態ＳＡ」にある。

一方、メモリカード１１２は、暗号化コンテンツデータのみを有しているため、そのままでは再生処理を行なうことができない。したがって、この時点ではメモリカード１１２は、「状態ＳＢ」にある。

メモリカード１１２が状態ＳＡとなるためには、改めてコンテンツサーバ１０から、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤやユーザＩＤデータ User－ＩＤ等の再生情報を取得する必要がある。

以上のような構成とすることで、メモリカードを有する正規のユーザのみがコンテンツデータ（音楽データ）を受信してメモリ中に格納することが可能となり、かつ、１度メモリカード中に格納されたデータを、他人にコピーさせる場合は、当該他人が再生可能な状態でデータを移植するためには、送信元においては、データの再生が不能となってしまう構成となっているので、無制限なコピーにより著作権が不当な不利益を被るのを防止することが可能となる。

なお、以上の説明では、コンテンツサーバ１０からの暗号化データを復号するための回路は、携帯電話機に着脱可能なメモリカード内に組み込まれる構成としたが、たとえば、携帯電話機内部に作りこまれる構成としてもよい。より一般には、情報サーバにアクセスする端末機器に着脱可能なメモリカード内に組み込ま

れる構成であってもよいし、当該端末機器にあらかじめ組み込まれる構成であってもよい。

［実施例２］

図１０は、本発明の実施例２のメモリカード１３０の構成を説明するための概略ブロック図であり、実施例１の図５と対比される図である。

実施例１のメモリカード１１０の構成と異なる点は、１つには、メモリカード１３０内にセッションキーＫｓを生成するためのセッションキー発生回路１４３２が設けられ、かつ、メモリカードという媒体に対応する公開暗号化キーＫＰｍｅｄｉａの値を保持するＫＰｍｅｄｉａ保持部１４４０が設けられていることである。メモリカード１３０は、これに応じて、セッションキー発生回路１４３２で生成されたセッションキーＫｓを、公開暗号化キーＫＰｍｅｄｉａにより暗号化してデータバスＢＳ３に与えるための暗号化処理部１４３０と、セッションキー発生回路１４３２からの出力と復号処理部１４０４との出力を受けて、選択的に暗号化処理部１４０６と復号処理部１４１０に与えるための切換えスイッチ１４３４を備える構成となっている。

切換えスイッチ１４３４は、接点Ｐｄ、Ｐｅ、Ｐｆを有し、接点Ｐｄ、Ｐｅには、復号処理部１４０４の出力が、接点Ｐｆにはセッションキー発生回路１４３２の出力が与えられる。切換えスイッチ１４３４は、それぞれ、接点Ｐｄ、Ｐｅ、Ｐｆに与えられる信号を、動作モードが、「配信モード」、「再生モード」、「移動モード」のいずれであるかに応じて、選択的に暗号化処理部１４０６と復号処理部１４１０に与える。

その他の構成は、図５に示した実施例１のメモリカード１１０の構成と同様であるの同一部分には同一符号を付して、その説明は繰り返さない。

メモリカード１３０の動作が、メモリカード１１０の動作と異なるのは、「移動」処理を行う場合である。

図１１は、メモリカード１３０の移動処理を説明するためのフローチャートであり、実施例１の図８と対比される図である。

図１１を参照して、まず、図１１においても、携帯電話機１００が送信側であり、携帯電話機１０２が受信側であるものとする。また、携帯電話機１０２にも、

メモリカード１３０と同様の構成を有するメモリカード１３２が装着されているものとする。

携帯電話機１００は、まず、自身の側のメモリカード１３０と、受信側の携帯電話機１０２に挿入されたメモリカード１３２に対して、移動リクエストを出力する（ステップＳ３００）。

さらに、携帯電話機１００においては、メモリカード１３０内のセッションキー発生回路１４３２は、セッションキーＫｓを生成し（ステップＳ３１２）、公開暗号化キーＫＰｍｅｄｉａを用いて、暗号化処理部１４３０がセッションキーＫｓを暗号化して（ステップＳ３１４）、たとえば、トランシーバモードではアンテナ１１０２を介して、暗号化されたセッションキーＫｓをカード１３２に伝達する（ステップＳ３１６）。

メモリカード１３２においては、復号処理部１４０４が、秘密復号キーＫｍｅｄｉａにより、セッションキーＫｓを復号抽出し（ステップＳ３２０）、さらに、セッションキーＫｓによりメモリカード１３２の公開暗号化キーＫＰｃａｒｄ（２）を暗号化して（ステップＳ３２２）、メモリカード１１０に対して、暗号化されたデータ［ＫＰｃａｒｄ（２）］Ｋｓを送信する（ステップＳ３２４）。

メモリカード１１０においては、メモリカード１１２から送信された暗号化データをセッションキーＫｓにより復号化して、メモリカード１１２の公開暗号化キーＫＰｃａｒｄ（２）を復号抽出する（ステップＳ３２６）。

以下の処理は、基本的に、図８で説明した実施例１の移動処理と同様であるのでその説明は繰り返さない。

以上のような処理を行なうと、ステップＳ３４２において、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータ User－ＩＤ等がカード１３０からは消去されているので、メモリカード１３０は「状態ＳＢ」となる。

一方、メモリカード１３２においては、暗号化コンテンツデータ以外にも、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤ等の再生情報が移動されているので、メモリカード１３２は「状態ＳＡ」となっている。

以上のような構成を用いることで、実施例１のメモリカードが奏する効果に加えて、たとえば、メモリカード１３０からメモリカード１３２へのデータの移動を、上述したようなセッションキー発生回路１５０２を有する携帯電話端末を介さずに、メモリカードとメモリカードとを接続可能なインタフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。

［実施例３］

図１２は、本発明の実施例３のメモリカード１４０の構成を説明するための概略ブロック図であり、実施例１の図５と対比される図である。

実施例１のメモリカード１１０の構成と異なる点は、メモリカード１４０内にコントローラ１４２０とデータの授受が可能なレジスタ１５００が設けられていることである。

その他の構成は、図５に示した実施例１のメモリカード５の構成と同様であるので同一部分には同一符号を付して、その説明は繰り返さない。

図１３は、図１２で説明したメモリカード１４０を用いた配信モードを説明するためのフローチャートである。

図１３においても、ユーザ１が、メモリカード１４０を用いることで、コンテンツサーバ１０からコンテンツデータの配信を受ける場合の動作を説明している。

まず、ユーザ１の携帯電話機１００から、ユーザのタッチキー１１０８の操作等によって、コンテンツサーバ１０に対して配信リクエストがなされる（ステップＳ１００）。

コンテンツサーバ１０においては、この配信リクエストに応じて、セッションキー発生部３１４が、セッションキーＫｓを生成する（ステップＳ１０３）。

続いて、コンテンツサーバ１０内の暗号化処理部３１６が、公開暗号化キーＫＰｍｅｄｉａにより、セッションキーＫｓを暗号化処理して、データバスＢＳ１に与える（ステップＳ１０４）。

通信装置３５０は、暗号化処理部３１６からの暗号化コンテンツデータ［Ｋｓ］Ｋｍｅｄｉａを、通信網を通じて、携帯電話機１００のメモリカード１４０に対して送信する（ステップＳ１０６）。

メモリカード１４０においては、メモリインタフェース１２００を介して、デ

ータバスＢＳ３に与えられた受信データを、復号処理部１４０４が、秘密復号キーＫｍｅｄｉａにより復号処理することにより、セッションキーＫｓを復号し抽出する（ステップＳ１０８）。

続いて、配信モードにおいては、切換えスイッチ１４０８は、接点Ｐａが閉じる状態が選択されているので、暗号化処理部１４０６は、接点Ｐａから与えられる公開暗号化鍵ＫＰｃａｒｄ（１）（ユーザ１のメモリカードにおける公開暗号化鍵）を、セッションキーＫｓにより暗号化して、データバスＢＳ３に与える。

携帯電話機１００は，暗号化処理部１４０６により暗号化されたデータ［ＫＰｃａｒｄ（１）］Ｋｓをコンテンツサーバ１０に対して出力する（ステップＳ１１２）。

コンテンツサーバ１０では、通信装置３５０により受信され、データバスＢＳ１に与えられたデータ［ＫＰｃａｒｄ（１）］Ｋｓを復号処理部３１８が、セッションキーＫｓにより復号化処理して、公開暗号化キーＫＰｃａｒｄ（１）を復号抽出する（ステップＳ１１４）。

続いて、配信制御部３１２は、ライセンスキーＫｃを配信情報データベース３０４より取得し（ステップＳ１１６）、かつ、配信情報データベース３０４等に保持されているデータを元に、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータ User－ＩＤ等のデータを生成する（ステップＳ１１８）。

暗号化処理部３２０は、配信制御部３１２からのライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータ User－ＩＤ等のデータを受取って、復号処理部３１８より与えられた公開暗号化キーＫＰｃａｒｄ（１）により暗号化処理する（ステップＳ１２０）。

暗号化処理部３２２は、暗号化処理部３２０により暗号化されたデータを受取って、さらにセッションキーＫｓにより暗号化して、データバスＢＳ１に与える（ステップＳ１２２）。

通信装置３５０は、暗号化処理部３２２により暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（１）］Ｋｓをカード１４０に対して送信する。

メモリカード１４０においては、復号処理部１４１０がセッションキーＫｓに

より、復号処理を行ない、データ［ＫＣ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（１）を抽出し（ステップＳ１２６）、メモリ１４１２に格納する（ステップＳ１２８）。

さらに、メモリカード１４０においては、復号処理部１４１６が、メモリ１４１２に格納されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（１）を復号し、復号されたデータＬｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤをコントローラ１４２０が、レジスタ１５００に格納する（ステップ１２９）。

一方、サーバ３０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを配信情報データベース３０４より取得して、通信装置３５０を介して、メモリカード１４０に送信する（ステップＳ１３０）。

メモリカード１４０においては、受信した暗号化コンテンツデータ［Ｄｃ］Ｋｃをそのままメモリ１４１２に格納する（ステップＳ１３２）。

以上のような動作により、メモリカード１４０は、音楽情報を再生可能な状態となる。

図１４は、携帯電話機１００内において、メモリカード１４０に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

図１４を参照して、携帯電話機のタッチキー１１０８等からのユーザ１の指示により、再生リクエストがメモリカード１４０に対して出力される（ステップＳ２００）。

メモリカード１４０では、コントローラ１４２０がレジスタ１５００からライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤ等を読出す（ステップＳ２０５）。

コントローラ１４２０は、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ等に含まれる情報に基づいて、復号可能なデータに対するリクエストであるかを判断し（ステップＳ２０６）、復号可能と判断した場合は、携帯電話機のコントローラ１１０６に対して、再生許可通知を送信する（ステップＳ２０８）。

携帯電話機１００においては、セッションキー発生回路１５０２がセッションキーＫｓを生成し（ステップＳ２１０）、暗号化処理部１５０４が、公開暗号化

キーＫＰｍｅｄｉａによりセッションキーＫｓを暗号化して（ステップＳ２１２）、データバスＢＳ２に暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａが出力される（ステップＳ２１４）。

メモリカード１４０は、データバスＢＳ２を介して、携帯電話機により生成された暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａを受け取り、公開暗号化キーＫｍｅｄｉａにより復号し、セッションキーＫｓを抽出する（ステップＳ２１６）。

続いて、メモリカード１４０は、メモリ１４１２から、暗号化されているデータ［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（１）を読出し、復号処理部１４１６が復号してライセンスキーＫｃを抽出する（ステップＳ２１８）。

続いて、抽出したセッションキーＫｓにより、ライセンスキーＫｃを暗号化し（ステップＳ２１９）、暗号化ライセンスキー［Ｋｃ］Ｋｓをデータバスｂｓ２に与える（ステップＳ２２０）。

携帯電話機１００の復号処理部１５０６は、セッションキーＫｓにより復号化処理を行なうことにより、ライセンスキーＫｃを取得する（ステップＳ２２２）。

続いて、メモリカード１４０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読出し、データバスＢＳ２に与える（ステップＳ２２４）。

携帯電話機の音楽再生部１５０８は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを、抽出されたライセンスキーＫｃにより復号処理し（ステップＳ２２６）、コンテンツデータを再生して混合部１５１０に与える（ステップＳ２２８）。

一方、ステップＳ２０６において、コントローラ１４２０が復号処理は不可能であると判断した場合、メモリカード１４０は、携帯電話機１００に対して、再生不許可通知を送信する（ステップＳ２３０）。

ステップＳ２３０の状態では、メモリカード１４０は、状態ＳＢにある。

図１５は、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なう処理を説明するためのフローチャートである。

まず、携帯電話機１００が送信側であり、携帯電話機１０２が受信側であるものとする。また、携帯電話機１０２にも、メモリカード１４０と同様の構成を有するメモリカード１４２が装着されているものとする。

携帯電話機１００は、まず、自身の側のメモリカード１４０と、受信側の携帯電話機１０２に挿入されたメモリカード１４２に対して、移動リクエストを出力する（ステップＳ３００）。

さらに、携帯電話機１００においては、セッションキー発生回路１５０２は、セッションキーＫｓを生成し（ステップＳ３０３）、公開暗号化キーＫＰｍｅｄｉａを用いて、暗号化処理部１５０４がセッションキーＫｓを暗号化して（ステップＳ３０４）、データバスＢＳ２を介して、メモリカード１４０に伝達し、さらに、たとえば、トランシーバモードではアンテナ１１０２を介して、暗号化されたセッションキーＫｓをメモリカード１４２に伝送する（ステップＳ３０６）。

メモリカード１４０においては、秘密復号キーＫｍｅｄｉａによりセッションキーＫｓを復号抽出する（ステップＳ３１８）。

同様にして、メモリカード１４２においても、秘密復号キーＫｍｅｄｉａにより、セッションキーＫｓを復号抽出し（ステップＳ３２０）、さらに、セッションキーＫｓによりカード１４２の公開暗号化キーＫＰｃａｒｄ（２）を暗号化して（ステップＳ３２２）、メモリカード１４０に対して、暗号化されたデータ［ＫＰｃａｒｄ（２）］Ｋｓを送信する（ステップＳ３２４）。

メモリカード１４０においては、メモリカード１４２から送信された暗号化データをセッションキーＫｓにより復号化して、メモリカード１４２の公開暗号化キーＫＰｃａｒｄ（２）を復号抽出する（ステップＳ３２６）。

続いて、メモリカード１４０においては、メモリ１４１２からメモリカード１４０の公開暗号化キーＫｃａｒｄ（１）により暗号化されているライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータUser－ＩＤが読出される（ステップＳ３２８）。

続いて、復号処理部１４１６が、秘密復号キーＫｃａｒｄ（１）により、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤとを復号処理する（ステップＳ３３０）。

コントローラ１４２０は、このようにして復号されたライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤの値を、レジスタ１５００内のデータ値と置換する（ステップＳ３３１）。

さらに、暗号化処理部１４１４は、復号処理部１４１０において抽出されたメモリカード１４２における公開暗号化キーＫＰｃａｒｄ（２）により、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータUser－ＩＤとを暗号化する（ステップＳ３３２）。

暗号化処理部１４１４により暗号化されたデータは、切換えスイッチ１４０８（接点Ｐｃが閉じている）を介して、さらに、暗号化処理部１４０６に与えられ、暗号化処理部１４０６は、データ［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（２）をセッションキーＫｓにより暗号化する（ステップＳ３３４）。

続いて、メモリカード１４０は、携帯電話機１００を介して、メモリカード１４２に対して、暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（２）］Ｋｓを送信する（ステップＳ３３６）。

メモリカード１４２においては、メモリカード１４０から送信されたデータを復号処理部１４１０により、セッションキーＫｓに基づいて復号化処理して、メモリ１４１２に格納する（ステップＳ３３９）。さらに、メモリカード１４２においては、復号処理部１４１６が、秘密復号キーＫｃａｒｄ（２）に基づいて、データ［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（２）を復号し、復号されたライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータUser－ＩＤをレジスタに格納する（ステップＳ３４１）。

一方、メモリカード１４０は、さらに、レジスタ１５００に格納されたライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータ User－ＩＤを消去する（ステップＳ３４３）。

続いて、メモリカード１４０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリから読出し、メモリカード１４２に対して送信する（ステップＳ３４４）。

メモリカード１４２は、受信した暗号化コンテンツデータをそのままメモリ１４１２に格納する（ステップＳ３４６）。

以上のような処理を行なうと、ステップＳ３４３において、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータ User－ＩＤがメモリカード１４０のレジスタ１５００からは消去されているので、メモリカード１４０は

「状態ＳＢ」となる。

一方、メモリカード１４２においては、暗号化コンテンツデータ以外にも、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤ等のすべてのデータが移動されているので、メモリカード１４２は「状態ＳＡ」となっている。

図１６は、図１２に示したメモリカード１４０において、携帯電話機１００から携帯電話機１０２へ、暗号化コンテンツデータの複製を行なう処理を説明するためのフローチャートである。

図１６を参照して、携帯電話機１００が、メモリカード１４０およびメモリカード１４２に対して複製リクエストを出力する（ステップＳ４００）。

続いて、メモリカード１４０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読出し、メモリカード１４２に対して送信する（ステップＳ４０２）。

メモリカード１４２においては、メモリカード１４０から送信された暗号化コンテンツデータを、そのままメモリ１４１２に記録する（ステップＳ４０４）。

以上のような動作を行なうと、メモリカード１４０には、暗号化されたコンテンツデータ、ライセンスキーＫｃ、ユーザＩＤデータ User－ＩＤ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ等のすべてのデータが残されているため、メモリカード１４０は再生可能な状態、すなわち、「状態ＳＡ」にある。

一方、メモリカード１４２は、暗号化コンテンツデータのみを有しているため、そのままでは再生処理を行なうことができない。したがって、この時点ではメモリカード１４２は、「状態ＳＢ」にある。

メモリカード１４２が状態ＳＡとなるためには、改めてコンテンツサーバ１０から、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤやユーザＩＤデータ User－ＩＤ等を取得する必要がある。

以上のような構成とすることで、実施例１のメモリカード１１０と同様の効果を奏する上に、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ等は、レジスタ１５００に格納され、コントローラ１４２０はそれを参照すればよいため、動作に必要な処理量を低減できる。

なお、以上の説明では、コンテンツサーバ１０からの暗号化データを復号するための回路は、携帯電話機に着脱可能なメモリカード内に組み込まれる構成としたが、たとえば、携帯電話機内部に作りこまれる構成としてもよい。より一般には、情報サーバにアクセスする端末機器に着脱可能なメモリカード内に組み込まれる構成であってもよいし、当該端末機器にあらかじめ組み込まれる構成であってもよい。

［実施例３の変形例］

実施例３のメモリカード１４０の再生処理では、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤにより復号処理が可能であるかを判断する構成であった。このライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤとしては、曲目の特定情報のみならず、再生回数の制限情報を含む構成とし、ユーザがコンテンツデータを再生できる回数を制限する構成とすることも可能である。特に、メモリカード１４０では、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤをレジスタ１５００に保持する構成としたので、以下に説明するように再生処理を行なうたびに、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤの内容を更新することが容易である。

以下に、このようなメモリカード１４０の再生処理を説明する。

図１７は、携帯電話機１００内において、実施例３の変形例のメモリカード１４０に保持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

図１７を参照して、携帯電話機のタッチキー１１０８等からのユーザ１の指示により、再生リクエストがメモリカード１４０に対して出力される（ステップＳ２００）。

メモリカード１４０では、コントローラ１４２０がレジスタ１５００からライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤ等を読出す（ステップＳ２０５）。

コントローラ１４２０は、復号化されたライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ等に含まれる情報に基づいて、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ中のデータにより指定されるコンテンツデータ（音楽データ）の再生処理の累算数が、再生可能回数の上限値を超えているかいないかを判断し（ステップＳ２

０６）、再生可能回数を超えていないと判断した場合は、携帯電話機のコントローラ１１０６に対して、再生許可通知を送信する（ステップＳ２０８）。

携帯電話機１００においては、セッションキー発生回路１５０２がセッションキーＫｓを生成し（ステップＳ２１０）、暗号化処理部１５０４が、秘密復号キーＫＰｍｅｄｉａによりセッションキーＫｓを暗号化して（ステップＳ２１２）、データバスＢＳ２に暗号化セッションキーデータ［Ｋｓ］Ｋｍｅｄｉａが出力される（ステップＳ２１４）。

メモリカード１４０は、データバスＢＳ２を介して、携帯電話機により生成された暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａを受け取り、秘密復号キーＫｍｅｄｉａにより復号し、セッションキーＫｓを抽出する（ステップＳ２１６）。

さらに、メモリカード１４０は、再生処理が行われることに応じて、レジスタ１５００中のライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤのうち、再生処理の累算数に関するデータを更新する（ステップ２１７）。

続いて、メモリカード１４０は、メモリ１４１２から、暗号化されているデータ［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（１）を読出し、復号処理部１４１６が復号してライセンスキーＫｃを抽出する（ステップＳ２１８）。

続いて、抽出したセッションキーＫｓにより、ライセンスキーＫｃを暗号化し（ステップＳ２１９）、暗号化ライセンスキー［Ｋｃ］Ｋｓをデータバスｂｓ２に与える（ステップＳ２２０）。

携帯電話機１００の復号処理部１５０６は、セッションキーＫｓにより復号化処理を行なうことにより、ライセンスキーＫｃを取得する（ステップＳ２２２）。

続いて、メモリカード１４０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読出し、データバスＢＳ２に与える（ステップＳ２２４）。

携帯電話機の音楽再生部１５０８は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを、抽出されたライセンスキーＫｃにより復号処理し（ステップＳ２２６）、コンテンツデータを再生して混合部１５１０に与える（ステップＳ２２８）。

一方、ステップＳ２０６において、コントローラ１４２０が復号処理は不可能であると判断した場合、メモリカード１４０は、携帯電話機１００に対して、再

生不許可通知を送信する（ステップＳ２３０）。

以上のような構成とすることで、ユーザがコンテンツデータを再生できる回数を制限することが可能である。

移動時には、再生情報内の再生回数を制限するライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤについて、メモリ１４１２に記録されたライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤを、レジスタ１５００にて再生の都度修正された再生回数を記録したライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤに変更して、新たな再生情報を構成する。このようにして、メモリカード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決められた再生回数の制限を越えることがないようにすることが可能である。

［実施例４］

図１８は、本発明の実施例４のメモリカード１５０の構成を説明するための概略ブロック図であり、実施例２の図１０と対比される図である。

実施例２のメモリカード１３０の構成と異なる点は、メモリカード１５０内にコントローラ１４２０とデータの授受が可能なレジスタ１５００が設けられていることである。

その他の構成は、図１０に示した実施例２のメモリカード１３０の構成と同様であるので同一部分には同一符号を付して、その説明は繰り返さない。

図１９は、メモリカード１５０の移動モードを説明するためのフローチャートであり、実施例２の図１１と対比される図である。

図１９を参照して、まず、図１９においても、携帯電話機１００が送信側であり、携帯電話機１０２が受信側であるものとする。また、携帯電話機１０２にも、メモリカード１５０と同様の構成を有するメモリカード１５２が装着されているものとする。

携帯電話機１００は、まず、自身の側のメモリカード１５０と、受信側の携帯電話機１０２に挿入されたメモリカード１５２に対して、移動リクエストを出力する（ステップＳ３００）。

さらに、携帯電話機１００においては、メモリカード１５０内のセッションキー発生回路１４３２は、セッションキーＫｓを生成し（ステップＳ３１２）、公

開暗号化キーＫＰｍｅｄｉａを用いて、暗号化処理部１４３０がセッションキーＫｓを暗号化して（ステップＳ３１４），たとえば、トランシーバモードではアンテナ１１０２を介して、暗号化されたセッションキーＫｓをカード１５２に伝達する（ステップＳ３１６）。

メモリカード１５２においても、復号処理部１４０４が、秘密復号キーＫｍｅｄｉａにより、セッションキーＫｓを復号抽出し（ステップＳ３２０）、さらに、セッションキーＫｓによりメモリカード１５２の公開暗号化キーＫＰｃａｒｄ（２）を暗号化して（ステップＳ３２２），メモリカード１５０に対して、暗号化されたデータ［ＫＰｃａｒｄ（２）］Ｋｓを送信する（ステップＳ３２４）。

メモリカード１５０においては、メモリカード１５２から送信された暗号化データをセッションキーＫｓにより復号化して、メモリカード１５２の公開暗号化キーＫＰｃａｒｄ（２）を復号抽出する（ステップＳ３２６）。

続いて、メモリカード１５０においては、メモリ１４１２からメモリカード１５０の公開暗号化キーＫｃａｒｄ（１）により暗号化されているライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータUser－ＩＤが読出される（ステップＳ３２８）。

続いて、復号処理部１４１６が、秘密復号キーＫｃａｒｄ（１）により、ライセンスキーＫｃ，ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤとを復号処理する（ステップＳ３３０）。

コントローラ１４２０は，このようにして復号されたライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤの値を、レジスタ１５００内のデータ値と置換する（ステップＳ３３１）。

さらに、暗号化処理部１４１４は、復号処理部１４１０において抽出されたメモリカード１５２における公開暗号化キーＫＰｃａｒｄ（２）により、ライセンスキーＫｃ，ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ，ユーザＩＤデータUser－ＩＤとを暗号化する（ステップＳ３３２）。

暗号化処理部１４１４により暗号化されたデータは、切換えスイッチ１４０８（接点Ｐｃが閉じている）を介して，さらに、暗号化処理部１４０６に与えられ、暗号化処理部１４０６は，データ［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－Ｉ

D］Ｋｃａｒｄ（２）をセッションキーＫｓにより暗号化する（ステップＳ３３４）。

続いて、メモリカード１５０は、携帯電話機１００を介して、メモリカード１５２に対して、暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（２）］Ｋｓを送信する（ステップＳ３３６）。

メモリカード１５２においては、メモリカード１５０から送信されたデータを復号処理部１４１０により、セッションキーＫｓに基づいて復号化処理して、メモリ１４１２に格納する（ステップＳ３３９）。さらに、メモリカード１５２は、秘密復号キーＫｃａｒｄ（２）に基づいて、データ［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（２）を復号し、復号されたライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤをレジスタ１５００に格納する（ステップＳ３４１）。

一方、メモリカード１５０は、さらに、レジスタ１５００に格納されたライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータ User－ＩＤを消去する（ステップＳ３４３）。

続いて、メモリカード１５０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリから読出し、メモリカード１５２に対して送信する（ステップＳ３４４）。

メモリカード１５２は、秘密復号キーをそのままメモリ１４１２に格納する（ステップＳ３４６）。

以上のような処理を行なうと、ステップＳ３４２において、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータ User－ＩＤ等がメモリカード１５０からは消去されているので、メモリカード１５０は「状態ＳＢ」となる。

一方、メモリカード１５２においては，暗号化されたコンテンツデータ以外にも、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤ等のすべてのデータが移動されているので、メモリカード１５２は「状態ＳＡ」となっている。

以上のような構成を用いることで、実施例２のメモリカード１３０が奏する効果に加えて、たとえば、メモリカード１５０からメモリカード１５２へのデータ

の移動を、上述したようなセッションキー発生回路１５０２を有する携帯電話機を介さずに、メモリカードとメモリカードとを接続可能なインタフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。

しかも、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ等は、レジスタ１５００に格納され、コントローラ１４２０はそれを参照すればよいため、動作に必要な処理量を低減できる。

さらに、ユーザがコンテンツデータを再生できる回数を制限する構成とすることも可能である。

［実施例５］

図２０は、本発明の実施例５のメモリカード１６０の構成を説明するための概略ブロック図であり、実施例３の図１２と対比される図である。

以下では、携帯電話機１００に装着されるメモリカード１６０の公開暗号化キーＫＰｍｅｄｉａと、携帯電話機１０２に装着されるメモリカード１６２の公開暗号化キーＫＰｍｅｄｉａとを区別して、それぞれ、メモリカード１６０に対するものを公開暗号化キーＫＰｍｅｄｉａ（１）と、メモリカード１６２に対するものを公開暗号化キーＫＰｍｅｄｉａ（２）と称することにする。

また、これに対応して、公開暗号化キーＫＰｍｅｄｉａ（１）で暗号化されたデータを復号可能であって、これとは非対称な秘密復号キーを秘密復号キーＫｍｅｄｉａ（１）と称し、公開暗号化キーＫＰｍｅｄｉａ（２）で暗号化されたデータを復号可能であって、これとは非対称な秘密復号キーを秘密復号キーＫｍｅｄｉａ（２）と称することにする。

このように、媒体固有の公開暗号化キーを区別することにより、以下の説明で明らかとなるように、メモリカードに複数の種類が存在する場合や、より一般的に、メモリカード以外の媒体がシステムのオプションとして存在する場合にも、対応することが可能となる。

図２０を参照して、本発明の実施例５のメモリカード１６０の構成が、実施例３のメモリカード１４０の構成と異なる点は、メモリカード１６０内にメモリカードという媒体に対応する公開暗号化キーＫＰｍｅｄｉａ（１）の値を保持し、データバスＢＳ３に公開暗号化キーＫＰｍｅｄｉａ（１）を出力するためのＫＰ

ｍｅｄｉａ保持部１４４０が設けられていることである。

その他の構成は、図１２に示した実施例３のメモリカード１４０の構成と同様であるので同一部分には同一符号を付して、その説明は繰り返さない。

図２１は、図２０で説明したメモリカード１６０を用いた配信モードを説明するためのフローチャートである。

図２１においても、ユーザ１が、メモリカード１６０を用いることで、コンテンツサーバ１０からの配信を受ける場合の動作を説明している。

まず、ユーザ１の携帯電話機１００から、ユーザのタッチキーの操作等によって、配信リクエストがなされる（ステップＳ１００）。

メモリカード１６０においては、この配信リクエストに応じて、ＫＰｍｅｄｉａ保持部１４４０から、公開暗号化キーＫＰｍｅｄｉａ（１）をコンテンツサーバ１０に対して送信する（ステップＳ１０１）。

コンテンツサーバ１０では、メモリカード１６０から転送された配信リクエストならびに公開暗号化キーＫＰｍｅｄｉａ（１）を受信すると（ステップＳ１０２）、セッションキー発生部３１４が、セッションキーＫｓを生成する（ステップＳ１０３）。

続いて、コンテンツサーバ１０内の暗号化処理部３１６が、公開暗号化キーＫＰｍｅｄｉａ（１）により、セッションキーＫｓを暗号化処理して、データバスＢＳ１に与える（ステップＳ１０４）。

通信装置３５０は、暗号化処理部３１６からの暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を、通信網を通じて、携帯電話機１００のメモリカード１６０に対して送信する（ステップＳ１０６）。

メモリカード１６０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた受信データを、復号処理部１４０４が、秘密復号キーＫｍｅｄｉａ（１）により復号処理することにより、セッションキーＫｓを復号し抽出する（ステップＳ１０８）。

以下の処理は、図１３において説明した実施例３のメモリカード１４０の動作と同様であるのでその説明は、繰り返さない。

このような構成とすることで、メモリカード自身が、セッションキーＫｓを送

る側（コンテンツサーバ１０）に、公開暗号化キーＫＰｍｅｄｉａ（１）を送信した上で、配信を受けることができ、メモリカード１６０は、コンテンツデータを再生可能な状態となる。

図２２は、携帯電話機１００内において、メモリカード１６０に保持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

図２２を参照して、携帯電話機のタッチキー１１０８等からのユーザ１の指示により、再生リクエストがメモリカード１６０に対して出力される（ステップＳ２００）。

メモリカード１６０においては、この再生リクエストに応じて、ＫＰｍｅｄｉａ保持部１４４０から、公開暗号化キーＫＰｍｅｄｉａ（１）を携帯電話機１００に対して送信する（ステップＳ２０１）。

携帯電話機１００では、メモリカード１６０からの公開暗号化キーＫＰｍｅｄｉａ（１）を受信して保持する（ステップＳ２０２）。

メモリカード１６０では、コントローラ１４２０がレジスタ１５００からライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ，ユーザＩＤデータ User－ＩＤ等を読出す（ステップＳ２０５）。

コントローラ１４２０は、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ等に含まれる情報に基づいて、復号可能なデータに対するリクエストであるかを判断し（ステップＳ２０６）、復号可能と判断した場合は、携帯電話機のコントローラ１１０６に対して、再生許可通知を送信する（ステップＳ２０８）。

携帯電話機１００においては、セッションキー発生回路１５０２がセッションキーＫｓを生成し（ステップＳ２１０）、暗号化処理部１５０４が、公開暗号化キーＫＰｍｅｄｉａ（１）によりセッションキーＫｓを暗号化して（ステップＳ２１２）、データバスＢＳ２に暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）が出力される（ステップＳ２１４）。

メモリカード１６０は、データバスＢＳ２を介して、携帯電話機により生成され、かつ暗号化されたセッションキーＫｓを受け取り、秘密復号キーＫｍｅｄｉａ（１）により復号し、セッションキーＫｓを抽出する（ステップＳ２１６）。

以下の処理は、図１４において説明した実施例３のメモリカード１４０の動作と同様であるのでその説明は、繰り返さない。

このような構成とすることで、メモリカード自身が、セッションキーＫｓを送る側（携帯電話機１００）に、公開暗号化キーＫＰｍｅｄｉａ（１）を送信した上で、再生動作を行なうことが可能となる。

図２３は、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なう処理を説明するためのフローチャートである。

まず、携帯電話機１００が送信側であり、携帯電話機１０２が受信側であるものとする。また、携帯電話機１０２にも、メモリカード１６０と同様の構成を有するメモリカード１６２が装着されているものとする。

携帯電話機１００は、まず、自身の側のメモリカード１６０と、受信側の携帯電話機１０２に挿入されたメモリカード１６２に対して、移動リクエストを出力する（ステップＳ３００）。

メモリカード１６０においては、公開暗号化キーＫＰｍｅｄｉａ（１）を携帯電話機１００に対して送信し（ステップＳ３０１）、メモリカード１６２においては、公開暗号化キーＫＰｍｅｄｉａ（２）を携帯電話機１００に対して送信する（ステップＳ３０１´）。

携帯電話機１００は、公開暗号化キーＫＰｍｅｄｉａ（１）および公開暗号化キーＫＰｍｅｄｉａ（２）を受信する（ステップ３０２）。

さらに、携帯電話機１００においては、セッションキー発生回路１５０２は、セッションキーＫｓを生成し（ステップＳ３０３）、公開暗号化キーＫＰｍｅｄｉａ（１）および公開暗号化キーＫＰｍｅｄｉａ（２）を用いて、暗号化処理部１５０４がセッションキーＫｓを暗号化する（ステップＳ３０４）。携帯電話機１００は、データバスＢＳ２を介して、メモリカード１６０に対しては暗号化セッションキー［Ｋｓ］ＫＰｍｅｄｉａ（１）を伝達し、さらに、たとえば、トランシーバモードではアンテナ１１０２を介して、暗号化セッションキー［Ｋｓ］ＫＰｍｅｄｉａ（２）をメモリカード１６２に伝達する（ステップＳ３０６）。

メモリカード１６０においては、秘密復号キーＫｍｅｄｉａ（１）によりセッションキーＫｓを復号抽出する（ステップＳ３１８）。

同様にして、メモリカード１６２においても、秘密復号キーＫｍｅｄｉａ（２）により、セッションキーＫｓを復号抽出する（ステップＳ３２０）。

以下の処理は、図１５において説明した実施例３のメモリカード１４０および１４２の動作と同様であるのでその説明は、繰り返さない。

このような構成とすることで、メモリカード自身が、セッションキーＫｓを送る側（携帯電話機１００）に、公開暗号化キーＫＰｍｅｄｉａ（１）およびＫＰｍｅｄｉａ（２）を送信した上で、移動モードを行なうことが可能となる。

なお、複製モードについては、メモリカード１６０および１６２の動作は、実施例３のメモリカード１４０および１４２の動作と同様である。

また、以上の説明では、レジスタ１５００が設けられているものとして説明したが、図５に示した実施例１のメモリカード１１０と同様に、レジスタ１５００が設けられていない構成とすることも可能である。

なお、以上の説明では、コンテンツサーバ１０からの暗号化データを復号するための回路は、携帯電話に着脱可能なメモリカード内に組み込まれる構成としたが、たとえば、携帯電話機内部に作りこまれる構成としてもよい。より一般には、情報サーバにアクセスする端末機器に着脱可能なメモリカード内に組み込まれる構成であってもよいし、当該端末機器にあらかじめ組み込まれる構成であってもよい。

さらに、図１７において説明した実施例３の変形例のメモリカードの動作と同様に、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤとして、曲目の特定情報のみならず、再生回数の制限情報を含む構成とし、ユーザがコンテンツデータを再生できる回数を制限する構成とすることも可能である。

［実施例６］

図２４は、本発明の実施例６のメモリカード１７０の構成を説明するための概略ブロック図であり、実施例４の図１８と対比される図である。

実施例４のメモリカード１５０の構成と異なる点は、第１のＫＰｍｅｄｉａ保持部１４４０が、データバスＢＳ３を介して他の媒体から送信された公開暗号化キー、たとえば、公開暗号化キーＫＰｍｅｄｉａ（２）を受信して保持し、暗号化処理部１４３０は、この公開暗号化キーＫＰｍｅｄｉａ（２）により、セッシ

ションキーＫｓを暗号化して、データバスＢＳ３に与える構成となっていることである。

さらに、メモリカード１７０は、自身に対応した公開暗号化キーＫＰｍｅｄｉａ（１）を保持して、データバスＢＳ３に出力することが可能な第２のＫＰｍｅｄｉａ保持部１４５０を備える構成となっている。

その他の構成は、図１８に示した実施例４のメモリカード１５０の構成と同様であるので同一部分には同一符号を付して、その説明は繰り返さない。

図２５は、メモリカード１７０の移動処理を説明するためのフローチャートであり、実施例４の図１９と対比される図である。

図２５を参照して、まず、図２５においても、携帯電話機１００が送信側であり、携帯電話機１０２が受信側であるものとする。また、携帯電話機１０２にも、メモリカード１７０と同様の構成を有するメモリカード１７２が装着されているものとする。

携帯電話機１００は、まず、自身の側のメモリカード１７０と、受信側の携帯電話機１０２に挿入されたメモリカード１７２に対して、移動リクエストを出力する（ステップＳ３００）。

メモリカード１７２は、第２のＫＰｍｅｄｉａ保持部１４５０から、自身に対応する公開暗号化キーＫＰｍｅｄｉａ（２）を携帯電話機１０２および１００を介して、メモリカード１７０に送信し（ステップＳ３０１）、メモリカード１７０は、公開暗号化キーＫＰｍｅｄｉａ（２）を受信して、第１のＫＰｍｅｄｉａ保持部１４４０に格納する（ステップＳ３０２）。

さらに、携帯電話機１００の側においては、メモリカード１７０内のセッションキー発生回路１４３２は、セッションキーＫｓを生成し（ステップＳ３１２）、公開暗号化キーＫＰｍｅｄｉａ（２）を用いて、暗号化処理部１４３０がセッションキーＫｓを暗号化して（ステップＳ３１４）、たとえば、トランシーバモードではアンテナ１１０２を介して、暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（２）をメモリカード１７２に伝達する（ステップＳ３１６）。

メモリカード１７２においては、復号処理部１４０４が、秘密復号キーＫｍｅｄｉａ（２）により、セッションキーＫｓを復号抽出する（ステップＳ３２０）。

以下の動作は、図１９に示したメモリカード１５０および１５２の動作と同様であるのでその説明は繰り返さない。

以上のような構成を用いることで、メモリカード１５０の種類に応じて、公開暗号化キーＫＰｍｅｄｉａの値が異なるような場合等においても、実施例４のメモリカードが奏する効果と同様に、たとえば、メモリカード１７０からメモリカード１７２へのデータの移動を、上述したようなセッションキー発生回路を有する携帯電話機を介さずに、メモリカードとメモリカードとを接続可能なインタフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。

しかも、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ等は、レジスタ１５００に格納され、コントローラ１４２０はそれを参照すればよいため、動作に必要な処理量を低減できる。

さらに、本実施例においても、ユーザがコンテンツデータを再生できる回数を制限する構成とすることも可能である。

なお、本実施例においても、図１０に示した実施例２のメモリカード１３０と同様に、レジスタ１５００を設けない構成とすることも可能である。

［実施例７］

実施例７のメモリカード１８０は、実施例４のメモリカード１５０の構成と異なって、配信サーバ、携帯電話機およびメモリカードの各々が、独自のセッションキーを生成する構成となっていることを１つの特徴とする。すなわち、配信サーバまたは携帯電話機の発生するセッションキーをＫｓとし、一方のメモリカード１８０の発生するセッションキーをＫｓ１とし、メモリカード１８０と同様の構成を有する他方のメモリカード１８２の発生するセッションキーをＫｓ２とする。

また、再生モードにおいて、携帯電話機側がメモリカードの生成するセッションキーを受け取るための公開暗号化キーをＫＰｐとし、この公開暗号化キーＫＰｐで暗号化されたデータを復号化できる秘密復号キーをＫｐとする。

図２６は、実施例７における携帯電話機１０１の構成を説明するための概略ブロック図である。